The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
ampleShop 2.1	Multiple vulnerabilities have been reported in ampleShop that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	ampleShop SQL Injection CVE-2006-2038	Not Available	Secunia, Advisory: SA19806, April 25, 2006

Bloggage	Multiple vulnerabilities have been reported in Bloggage, 'check_login.asp', that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	Bloggage SQL Injection CVE-2006-2010	7.0	Secunia, Advisory: SA19751, April 21, 2006
HP StorageWorks Secure Path for Windows 4.0C-SP2	A vulnerability has been reported in StorageWorks Secure Path for Windows that could let remote malicious users cause a Denial of Service. HP Currently we are not aware of any exploits for this vulnerability.	HP StorageWorks Secure Path for Windows Denial Of Service	Not Available	Security Tracker, Alert ID: 1015969, April 20, 2006
iOpus Secure Email Attachments	A vulnerability has been reported in iOpus Secure Email Attachments, insecure encryption, that could let remote malicious users disclose encrypted information. No workaround or patch available at time of publishing. There is no exploit code required.	iOpus Secure Email Attachments Information Disclosure CVE-2006-2036	Not Available	Security Tracker, Alert ID: 1015980, April 24, 2006
Ivan Zahariev IZArc 3.5 beta 3	Multiple input validation vulnerabilities have been reported in IZArc that could let remote malicious users traverse directories. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	IZArc Directory Traversal CVE-2006-2006	2.3	Secunia, Advisory: SA19791, April 24, 2006
Microsoft Internet Explorer 6.0 SP2	A vulnerability has been reported in Internet Explorer, 'object' tag memory corruption, that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2006-1992	8.0	Secunia, Advisory: SA19762, April 22, 2006
Microsoft Outlook Express	A vulnerability has been reported in Outlook Express that could let remote malicious users execute arbitrary code. Microsoft **V1.2: Revised due to issues discovered with the security update.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Outlook Express Arbitrary Code Execution CVE-2006-0014	**5.6**	Microsoft, Security Bulletin MS06-016, April 11, 2006 US-CERT VU#234812 **Microsoft, Security Bulletin MS06-016 V1.2, April 26, 2006**
Microsoft Windows Explorer	A vulnerability has been reported in Windows Explorer, COM Object handling, that could let remote malicious users execute arbitrary code. Microsoft **V2.0: Revised to inform customers that revised versions of the security update are available.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Explorer Arbitrary Code Execution CVE-2006-0012	**5.6**	Microsoft, Security Bulletin MS06-015, April 11, 2006 US-CERT VU#641460 **Microsoft, Security Bulletin MS06-015 V2.0, April 25, 2006**
Pablo Software Solutions Quick 'n Easy FTP Server 1.60 through 1.71, 3.0	A buffer overflow vulnerability has been reported in Quick 'n Easy FTP Server that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Quick 'n Easy FTP Server Arbitrary Code Execution CVE-2006-2027	Not Available	Security Focus, ID: 17681, April 24, 2006

Skulltag 0.96f	A vulnerability has been reported in Skulltag that could let remote malicious users cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit, skulltagfs.zip, has been published.	Skulltag Denial of Service or Arbitrary Code Execution CVE-2006-2012	2.3	Secunia, Advisory: SA19767, April 24, 2006
SolarWinds TFTP Server 5.0.55, 5.0.60, 8.1	An input validation vulnerability has been reported in TFTP Server that could let remote malicious users traverse directories. SolarWinds TFTP Server 8.2 There is no exploit code required.	SolarWinds TFTP Server Directory Traversal Vulnerability CVE-2006-1951	2.3	Security Focus, ID: 17648, April 21, 2006
SpeedProject Squeez 5.10 Build 4460, SpeedCommander 10.52 build 4450, SpeedCommander 11.01 build 4450	A buffer overflow vulnerability has been reported in SpeedProject products, ACE archive handling, that could let remote malicious users execute arbitrary code execution. SpeedProject There is no exploit code required.	SpeedProject Multiple Arbitrary Code Execution	Not Available	Secunia, Advisory: SA19473, April 26, 2006
Sybase Pylon Anywhere 5.5.4, 6.2.1, 6.3.2, 6.4.2, 6.4.9	A vulnerability has been reported in Pylon Anywhere that could let remote malicious uses disclose information. Sybase Currently we are not aware of any exploits for this vulnerability.	Sybase Pylon Anywhere Information Disclosure CVE-2006-1997	1.6	Security Focus, ID: 17677, April 24, 2006
Winny 2.0 b5.7, 2.0 b7.1	A heap overflow vulnerability has been reported in Winny that could let remote malicious users to execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Winny Arbitrary Code Execution CVE-2006-2007	7.0	Security Focus, ID: 17666, April 24, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
(LS)3 Fenice 1.10	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported when parsing an RTSP URL received from a client due to a boundary error, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to an input validation error when handling the Content-Length HTTP header received from a client. No workaround or patch available at time of publishing. Proof of Concept exploits and an exploit script, fenice.c, have been published.	Fenice Remote Buffer Overflow & Denial of Service CVE-2006-2022 CVE-2006-2023	7.0 (CVE-2006-2022) 2.3 (CVE-2006-2023)	Security Focus, Bugtraq ID: 17678, April 24, 2006
4homepages 4images 1.7	A Cross-Site Scripting vulnerability has been reported in 'register.php' ' due to insufficient sanitization of the 'user_name' parameter before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	4homepages 4images Cross-Site Scripting CVE-2006-2011	1.9	Secunia Advisory: SA19745, April 21, 2006

Apple Safari 2.0-2.0.3, Mac OS X Server 10.4-10.4.6, 10.3-10.3.9, OS X 10.4-10.4.6, 10.3-10.3.9	Multiple vulnerabilities have been reported which could let a remote malicious user cause a Denial of Service or execute arbitrary code: a vulnerability was reported in the 'BOMStackPop()' function in the 'BOMArchiveHelper' when decompressing malformed ZIP archives, a vulnerability was reported in the 'KWQListIteratorImpl(),' 'drawText(),' and 'objc_msgSend_rtp()' functions in Safari when processing malformed HTML tags; a vulnerability was reported in the 'ReadBM()' function when processing malformed BMP images; a vulnerability was reported in the 'CFAllocatorAllocate()' function when processing malformed GIF images; and a vulnerability was reported in the '_cg_TIFFSetField()' and 'PredictorVSetField()' functions when processing malformed TIFF images. No workaround or patch available at time of publishing. Proof of Concept exploits have been reported.	Mac OS X Multiple Potential Vulnerabilities CVE-2006-1982 CVE-2006-1983 CVE-2006-1984 CVE-2006-1985 CVE-2006-1986 CVE-2006-1987 CVE-2006-1988	7.0 (CVE-2006-1982) 4.7 (CVE-2006-1983) 2.3 (CVE-2006-1984) 1.6 (CVE-2006-1985) 7.0 (CVE-2006-1986) 7.0 (CVE-2006-1987) 2.3 (CVE-2006-1988)	Secunia Advisory: SA19686, April 21, 2006
Apple Safari 2.0.3, 1.3.1	A remote Denial of Service vulnerability has been reported in the 'rowspan' attribute when processing 'td' HTML tags that contain overly large values. No workaround or patch available at time of publishing. An exploit script, safari-dos.txt, has been published.	Apple Safari Web Browser Rowspan Denial of Service CVE-2006-2019	2.3	Security Tracker Alert ID: 1015982, April 24, 2006
CrossFire CrossFire 1.8.0 & prior	A remote Denial of Service vulnerability has been reported in the 'oldsocketmode' option due to an error. Updates available **Gentoo** There is no exploit code required.	CrossFire Remote Denial of Service CVE-2006-1010	4.7	Secunia Advisory: SA19044, February 28, 2006 **Gentoo Linux Security Advisory, GLSA 200604-11, April 22, 2006**
Cyrus SASL Cyrus SASL Library 2.x	A remote Denial of Service vulnerability has been reported due to an unspecified error during DIGEST-MD5 negotiation. Update to version 2.1.21. **Gentoo** **Ubuntu** **Debian** Currently we are not aware of any exploits for this vulnerability.	Cyrus SASL Remote Digest-MD5 Denial of Service CVE-2006-1721	**1.9**	Secunia Advisory: SA19618, April 11, 2006 **Gentoo Linux Security Advisory, GLSA 200604-09, April 21, 2006** **Ubuntu Security Notice, USN-272-1, April 24, 2006** **Debian Security Advisory, DSA-1042-1, April 25, 2006**
Dan Littlejohn Asterisk Recording Interface 0.7.15	A buffer overflow vulnerability has been reported in 'audio.php' due to a signedness error in 'format_jpeg.c' when processing an overly large JPEG image, which could let a remote malicious user execute arbitrary code. Update available Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Asterisk JPEG Image Handling Buffer Overflow CVE-2006-1827	4.7	Secunia Advisory: SA19800, April 24, 2006
Dnsmasq Dnsmasq 2.29	A remote Denial of Service vulnerability has been reported when a 'broadcast reply' request is submitted to the server. Update available There is no exploit code required.	DNSmasq Broadcast Reply Denial of Service CVE-2006-2017	2.3	Security Focus, Bugtraq ID: 17662, April 24, 2006
fbida fbida 2.03, 2.01	A vulnerability has been reported in the 'fbgs' script because temporary files are created insecurely when the 'TMPDIR' environment variable isn't defined, which	Fbida FBGS Insecure Temporary File Creation	1.3	Secunia Advisory: SA19559, April 10, 2006 **Gentoo Linux Security**

	could let a remote malicious user create/overwrite arbitrary files. **Gentoo** There is no exploit code required.	CVE-2006-1695		**Advisory, GLSA 200604-13, April 23, 2006**
Free RADIUS FreeRADIUS 1.0-1.0.5	A vulnerability has been reported in the EAP-MSCHAPv2 state machine due to an error, which could let a malicious user bypass authentication and cause a Denial of Service. Updates available SuSE RedHat Gentoo **SGI** Currently we are not aware of any exploits for this vulnerability.	FreeRADIUS EAP-MSCHAPv2 Authentication Bypass CVE-2006-1354	8.0	Security Focus, Bugtraq ID: 17171, March 21, 2006 SUSE Security Announcement, SUSE-SA:2006:019, March 28, 2006 RedHat Security Advisory, RHSA-2006:0271-11, April 4, 2006 Gentoo Linux Security Advisory, GLSA 200604-03, April 4, 2006 **SGI Security Advisory, 20060404-01-U, April 24, 2006**
IPsec-Tools IPsec-Tools0.6-0.6.2, 0.5-0.5.2	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions when in 'AGGRESSIVE' mode. IpsecTools Ubuntu Gentoo SUSE Conectiva Mandriva Debian **RHSA-2006-0267** Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	IPsec-Tools ISAKMP IKE Remote Denial of Service CVE-2005-3732	5.0	Security Focus, Bugtraq ID: 15523, November 22, 2005 Ubuntu Security Notice, USN-221-1, December 01, 2005 Gentoo Linux Security Advisory, GLSA 200512-04, December 12, 2005 SUSE Security Announcement, SUSE-SA:2005:070, December 20, 2005 Conectiva Linux Announcement, CLSA-2006:1058, January 2, 2006 Mandriva Security Advisory, MDKSA-2006:020, January 25, 2006 Debian Security Advisory, DSA-965-1, February 6, 2006 **RedHat Security Advisory, RHSA-2006:0267-11, April 25, 2006**
ISC BIND 4.x.x, 8.x.x, 9.2.x, 9.3.x	A remote Denial of Service vulnerability has been reported due to a failure to properly handle malformed TSIG (Secret Key Transaction Authentication for DNS) replies. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	ISC BIND TSIG Zone Transfer Remote Denial of Service	Not Available	Security Focus, Bugtraq ID: 17692, April 25, 2006
KRANKIKOM GmbH ContentBoxX 0	A Cross-Site Scripting vulnerability has been reported in 'login.php' due to insufficient sanitization of the 'action'	ContentBoxx Cross-Site Scripting	2.3	Secunia Advisory: SA19733, April 20, 2006

parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	CVE-2006-1971

Multiple Vendors Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36	Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor::StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream::readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code. Patches available Fedora RedHat KDE SUSE Ubuntu Gentoo RedHat RedHat RedHat Mandriva Debian Debian Debian Fedora SuSE RedHat SGI Debian TurboLinux Debian Debian Slackware Slackware Gentoo SGI SCO **SCOSA-2006.20**	Xpdf Buffer Overflows CVE-2005-3191 CVE-2005-3192 CVE-2005-3193	3.9 (CVE-2005-3191) 7.0 (CVE-2005-3192) 3.9 (CVE-2005-3193)	iDefense Security Advisory, December 5, 2005 Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005 RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005 KDE Security Advisory, advisory-20051207-1, December 7, 2005 SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005 Ubuntu Security Notice, USN-227-1, December 12, 2005 Gentoo Linux Security Advisory, GLSA 200512-08, December 16, 2005 RedHat Security Advisories, RHSA-2005:868-4, RHSA-2005:867-5 & RHSA-2005:878-4, December 20, 2005 Mandriva Linux Security Advisories MDKSA-2006:003-003-006, January 6, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 Debian Security Advisory, DSA-937-1, January 12, 2006 Debian Security Advisory, DSA 938-1, January 12, 2006 Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006 SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006 RedHat Security Advisory, RHSA-2006:0160-14, January 19, 2006 SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006 SGI Security Advisory, 20051201-01-U, January 20, 2006 Debian Security Advisory, DSA-950-1, January 23, 2006 Turbolinux Security Advisory, TLSA-2006-2, January 25, 2006 Debian Security Advisories, DSA-961-1 & 962-1, February 1, 2006 Slackware Security Advisories, SSA:2006-045-04 & SSA:2006-045-09, February 14, 2006 Gentoo Linux Security Advisory, GLSA 200603-02, March 4, 2006

	SCOSA-2006.21 Currently we are not aware of any exploits for these vulnerabilities.			SGI Security Advisory, 20060201-01-U, March 14, 2006 SCO Security Advisory, SCOSA-2006.15, March 22, 2006 **SCO Security Advisories, SCOSA-2006.20 & SCOSA-2006.21, April 18, 2006**
Multiple Vendors Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha; 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; abc2ps 1.3.3	Multiple buffer overflow vulnerabilities have been reported when processing ABC music files due to various boundary errors, which could let a remote malicious user execute arbitrary code. Debian Currently we are not aware of any exploits for these vulnerabilities.	abc2ps ABC Music File Buffer Overflows CVE-2006-1513	5.6	Security Focus, Bugtraq ID: 17689, April 25, 2006 Debian Security Advisory, DSA-1041-1, April 25, 2006
Multiple Vendors Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha; Blender 2.36	A vulnerability has been reported due to a failure to sanitize user-supplied input before using in a Python 'eval' statement, which could let a remote malicious user execute arbitrary python code. Blender Debian Proof of Concept exploits have been published.	Blender BVF File Import Python Code Execution CVE-2005-3302	7.0	Debian Security Advisory, DSA-1039-1, April 24, 2006
Multiple Vendors Linux Kernel 2.6.x	A Denial of Service vulnerability has been reported in the '_keyring_search_one()' function when a key is added to a non-keyring key. Update to version 2.6.16.3 or later. **Fedora** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel '__keyring_search_one' Denial of Service CVE-2006-1522	2.3	Secunia Advisory: SA19573, April 11, 2006 **Fedora Update Notifications, FEDORA-2006-421, FEDORA-2006-423, April 19 & 20, 2006**
Multiple Vendors Linux Kernel 2.6.x	A vulnerability has been reported because AMD K7/K8 CPUs only save/restore certain x87 registers in FXSAVE instructions when an exception is pending, which could let a remote malicious user obtain sensitive information. Updates available FreeBSD **Fedora** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel x87 Register Information Leak CVE-2006-1056	**1.6**	Secunia Advisory: SA19724, April 19, 2006 FreeBSD Security Advisory, FreeBSD-SA-06:14, April 19, 2006 **Fedora Update Notifications, FEDORA-2006-421, FEDORA-2006-423, April 19 & 20, 2006**
Multiple Vendors Linux kernel 2.6-2.6.16	A Denial of Service vulnerability has been reported when program control is returned using SYSRET on Intel EM64T CPUs. Updates available **Fedora** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Intel EM64T SYSRET Denial of Service CVE-2006-0744	1.6	Secunia Advisory: SA19639, April 17, 2006 **Fedora Update Notifications, FEDORA-2006-421, FEDORA-2006-423, April 19 & 20, 2006**
Multiple Vendors Linux kernel 2.6-2.6.16, 2.5-2.5.69, 2.4-2.4.33	A vulnerability has been reported regarding shared memory access, which could let a malicious user bypass security restrictions. Patches available **Fedora** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Shared Memory Security Restriction Bypass CVE-2006-1524	**3.3**	Security Focus, Bugtraq ID: 17587, April 18, 2006 **Fedora Update Notifications, FEDORA-2006-421, & FEDORA-2006-423, April 19 & 20, 2006**

Multiple Vendors Linux Kernel prior to 2.6.16.8	A Denial of Service vulnerability has been reported in the 'ip_route_input()' function when requesting a multi-cast IP address. Updates available **Fedora** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IP_ROUTE_INPUT Denial of Service CVE-2006-1525	**2.3**	Secunia Advisory: SA19709, April 19, 2006 **Fedora Update Notifications, FEDORA-2006-421, & FEDORA-2006-423, April 19 & 20, 2006**

Multiple Vendors
RedHat Fedora Core5, Core4;
GNOME GDM 2.14.1;
Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha
	A vulnerability has been reported in GDM gdm due to the way permissions on the '.ICEauthority' file are modified, which could let a remote malicious user obtain sensitive information.
	This issue has been addressed in the latest CVS repository.
	Vulnerability may be exploited with standard utilities and applications.
		GNOME Foundation GDM .ICEauthority Improper File Permissions
		CVE-2006-1057
			3.9	Security Focus, Bugtraq ID: 17635, April 20, 2006

Multiple Vendors RedHat Fedora Core5; Beagle prior to 0.2.5	A vulnerability has been reported due to the insecure construction of command line arguments that are passed to external helper applications, which could let a remote malicious user execute arbitrary code. Updates available Fedora There is no exploit code required.	Beagle Helper Applications Arbitrary Code Execution CVE-2006-1865	7.0	Secunia Advisory: SA19778, April 25, 2006
Multiple Vendors Trustix Secure Linux 3.0, 2.2; Linux kernel 2.6.12 up to versions before 2.6.17-rc1	A Denial of Service vulnerability has been reported in the 'fill_write_buffer()' function due to an out-of-bounds memory error. Update to version 2.6.16.2. **Fedora** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS Denial of Service CVE-2006-1055	2.3	Secunia Advisory: SA19495, April 10, 2006 **Fedora Update Notifications, FEDORA-2006-421, FEDORA-2006-423, April 19 & 20, 2006**
Multiple Vendors Trustix Secure Linux 3.0; Linux kernel 2.6-2.6.16	A vulnerability has been reported in the '__group_ complete_signal' function of the RCU signal-handling facility. The impact was not specified. A patch is available from the vendor. Currently we are not aware of any exploits for this vulnerability.	Linux Kernel RCU signal 'handling __group_ complete_signal' Function CVE-2006-1523	4.9	Security Focus, Bugtraq ID: 17640, April 21, 2006
Multiple Vendors XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo RHSA-2005-329.html RHSA-2005-396.htm Ubuntu Mandriva Fedora Trustix Debian Sun SUSE Slackware Sun SUSE	XFree86 Pixmap Allocation Buffer Overflow CVE-2005-2495	3.9	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441 Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Debian Security Advisory DSA 816-1, September 19, 2005

	Avaya Sun 101926: Updated Contributing Factors, Relief/Workaround, and Resolution sections. NetBSD SGI **SCOSA-2006.22** Currently we are not aware of any exploits for this vulnerability.			Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005 SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005 Slackware Security Advisory, SSA:2005-269-02, September 26, 2005 Sun(sm) Alert Notification Sun Alert ID: 101953, October 3, 2005 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Avaya Security Advisory, ASA-2005-218, October 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, Updated October 24, 2005 NetBSD Security Update, October 31, 2005 SGI Security Advisory, 20060403-01-U, April 11, 2006 **SCO Security Advisory, SCOSA-2006.22, April 21, 2006**
Multiple Vendors xzgv Image Viewer 0.8 0.7, 0.6; SuSE Linux Professional 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1	A buffer overflow vulnerability has been reported when processing JPEG files due to a boundary error, which could let a remote malicious user execute arbitrary code. SuSE **Gentoo** **dsa-1037** **dsa-1038** Currently we are not aware of any exploits for this vulnerability.	XZGV Image Viewer Remote Buffer Overflow CVE-2006-1060	7.0	SUSE Security Summary Report Announcement, SUSE-SR:2006:008, April 7, 2006 **Gentoo Linux Security Advisory, GLSA 200604-10, April 21, 2006** **Debian Securities, Advisory,DSA-1037-1, DSA-1038-1, April 21 & 22, 2006**

Multiple Vendors
Yukihiro Matsumoto Ruby 1.8-1.8.2, 1.6 - 1.6.8;
Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0.4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
RedHat Fedora Core1-Core4, Enterprise Linux WS 4, ES 4, Enterprise Linux Desktop version 4, Enterprise Linux AS 4
	A remote Denial of Service vulnerability has been reported in the WEBrick HTTP server due to the use of blocking network operations.
	Ruby
	Ubuntu
	Mandriva
	Vulnerability may be with standard network utilities; however, a Proof of Concept exploit has been published.
		Yukihiro Matsumoto Ruby XMLRPC Server Remote Denial of Service
		CVE-2006-1931
			2.3	Security Focus, Bugtraq ID: 17645, April 21, 2006
				Ubuntu Security Notice, USN-273-1, April 24, 2006
				Mandriva Security Advisory, MDKSA-2006:079, April 25, 2006

Net Clubs Pro Net Clubs Pro 4.0	Cross-Site Scripting vulnerabilities have been reported in '/vchat/scripts/sendim.cgi' due to insufficient sanitization of the 'onuser,' 'pass,' 'chatsys,' 'room,' 'username,' and 'to' parameters, in 'vchat/scripts/imessge.cgi' due to insufficient sanitization of the 'username' parameter, and in 'login.cgi' due to insufficient sanitization of the 'password' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time	Net Clubs Pro Multiple Cross-Site Scripting CVE-2006-1965	4.7	Secunia Advisory: SA19651, April 20, 2006

	of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.			
pdnsd pdnsd prior to 1.2.4	A remote Denial of Service vulnerability has been reported due to a failure to properly handle DNS queries. Updates available Currently we are not aware of any exploits for this vulnerability.	PDNSD DNS Query Remote Denial of Service	Not Available	Secunia Advisory: SA19835, April 26, 2006
Sendmail Consortium Sendmail prior to 8.13.6: **Sun Cobalt RaQ 4, RaQ 550, RaQ XTR**	A vulnerability has been reported due to a race condition caused by the improper handling of asynchronous signals, which could let a remote malicious user execute arbitrary code. Updates available RHSA-2006:0264-8 RHSA-2006:0265-9 Fedora Gentoo AIX Sun SuSE FreeBSD Slackware OpenBSD Avaya Debian HP NetBSD SGI F-Secure SGI **Sun** A Proof of Concept exploit script, sendtest.c, has been published.	Sendmail Asynchronous Signal Handling Remote Code Execution CVE-2006-0058	8.0	Internet Security Systems Protection Advisory, March 22, 2006 Technical Cyber Security Alert TA06-081A US-CERT VU#834865 RedHat Security Advisories, RHSA-2006:0264-8 & RHSA-2006:0265-9, March 22, 2006 Sun(sm) Alert Notification Sun Alert ID: 102262, March 24, 2006 Gentoo Linux Security Advisory, GLSA 200603-21, March 22, 2006 SUSE Security Announcement, SUSE-SA:2006:017, March 22, 2006 FreeBSD Security Advisory, FreeBSD-SA-06:13, March 22, 2006 Slackware Security Advisory, SSA:2006-081-01, March 22, 2006 Avaya Security Advisory, ASA-2006-074, March 24, 2006 Debian Security Advisory, DSA-1015-1, March 24, 2006 HP Security Bulletin, HPSBUX02108, March 27, 2006 NetBSD Security Advisory, /NetBSD-SA2006-010, March 28, 2006 SGI Security Advisory, 20060302-01-P, March 22, 2006 F-Secure Security Bulletin, FSC-2006-2, March 28, 2006 SGI Security Advisory, 20060401-01-U, April 4, 2006 **Sun(sm) Alert Notification Sun Alert ID: 102324, April 25, 2006**
Sun Microsystems Inc. Solaris 10_x86, 10	A vulnerability has been reported in the 'getpwnam()' family of non-reentrant functions due to a failure of the PKCS#11 library to properly utilize non-reentrant functions, which could let a malicious user obtain elevated privileges. Patches available	Sun Solaris PKCS#11 Library Elevated Privileges CVE-2006-2064	Not Available	Sun Alert ID: 102316, April 24, 2006

	Currently we are not aware of any exploits for this vulnerability.			
Tcpick Tcpick 0.2.1	A remote Denial of Service vulnerability has been reported in 'write.c' due to a failure to handle malformed input. No workaround or patch available at time of publishing. Vulnerability may be exploited with readily available network utilities.	Tcpick Remote Denial of Service CVE-2006-0048	Not Available	Security Focus, Bugtraq ID: 17665, April 24, 2006
University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g Trustix Debian Gentoo SUSE Mandriva Slackware Conectiva RedHat RedHat Fedora Trustix SGI **RHSA-2006-0267** Currently we are not aware of any exploits for this vulnerability.	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	7.0	Secunia, Advisory: SA17062, October 5, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005 Debian Security Advisory, DSA 861-1, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 US-CERT VU#933601 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194, October 21 & 26, 2005 Slackware Security Advisory, SSA:2005-310-06, November 7, 2005 Conectiva Linux Announcement, CLSA-2005:1046, November 21, 2005 RedHat Security Advisory, RHSA-2005:848-6 & 850-5, December 6, 2005 Fedora Update Notifications, FEDORA-2005-1112 & 1115, December 8, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0074, December 23, 2005 SGI Security Advisory, 20051201-01-U, January 20, 2006 **RedHat Security Advisory, RHSA-2006:0267-11, April 25, 2006**
UPDI Network Enterprise @1 Event Publisher	Several vulnerabilities have been reported: an HTML injection vulnerability was reported in 'event-publisher_ admin.htm' and 'eventpublisher_ usersubmit.htm' due to insufficient sanitization of the 'Event,' 'Description,' 'Time,' 'Website,' and 'Public Remarks' fields before using, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to insufficient restriction of 'eventpublisher.txt' which could lead to the disclosure of sensitive information. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	@1 Event Publisher HTML Injection & Information Disclosure CVE-2006-1436 CVE-2006-1437	2.3 (CVE-2006-1436) 2.3 (CVE-2006-1437)	Secunia Advisory: SA19727, April 21, 2006

UPDI Network Enterprise @1 Table Publisher 2006.3.23	An HTML injection vulnerability has been reported due to insufficient sanitization of the 'Title of table' field when adding a new table, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	@1 Table Publisher HTML Injection CVE-2006-1795	1.9	Secunia Advisory: SA19723, April 21, 2006

[back to top]

Multiple Operating Systems - Windows/UNIX/Linux/Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
3Com Baseline Switch 2848-SFP Plus 1.0.2	A remote Denial of Service vulnerability has been reported due to an error when handling DHCP packets. Update available There is no exploit code required.	3Com Baseline Switch 2848-SFP Plus Remote Denial of Service CVE-2006-2054	Not Available	Secunia Advisory: SA19756, April 25, 2006
AspSitem AspSitem 1.83 & prior	An SQL injection vulnerability has been reported in 'haberler.asp' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Update available Vulnerability can be exploited through a web client; however, an exploit script, aspsitem.pl, has been published.	AspSitem SQL Injection CVE-2006-1964	7.0	Secunia Advisory: SA19693, April 20, 2006
built2go built2go Movie Review 2B & prior	A file include vulnerability has been reported in 'Movie_CLS.PHP3' due to insufficient sanitization of the 'full_path' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, built2go.rfi.txt, has been published.	Built2go Movie Review Remote File Include CVE-2006-2008	7.0	Secunia Advisory: SA19749, April 24, 2006
Cartweaver Cartweaver 2.16.11	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported in 'Results.cfm' due to insufficient sanitization of the 'category' parameter and in 'Details.cfm' due to insufficient sanitization of the 'ProdID' parameter, which could let a remote malicious user execute arbitrary SQL code; and it is also possible to reveal installation path by passing invalid parameter values to 'Results.cfm,' 'Details.cfm,' and 'Results.cfm.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Cartweaver SQL Injection & Path Disclosure CVE-2006-2046 CVE-2006-2047	Not Available	Secunia Advisory: SA19812, April 26, 2006
Cisco Linksys RT31P2 VoIP Router 0	Remote Denials of Service vulnerabilities have been reported when processing malformed SIP (Session Initiation Protocol) messages due to various errors. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Linksys RT31P2 Remote Denials of Service CVE-2006-1973	2.3	US-CERT VU#621566
CoreNews CoreNews 2.0.1	Multiple input validation vulnerabilities have been reported including a remote file include vulnerability and an SQL injection vulnerability due to insufficient sanitization of user-supplied input, which could lead to the execution of arbitrary SQL and PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploit scripts,	CoreNews Multiple Input Validation CVE-2006-2032 CVE-2006-2033	Not Available	Security Focus, Bugtraq ID: 17655, April 22, 2006

	17655-exploit.pl and 17655.html, have been published.			
David Zhong logMethods 0.9	A Cross-Site Scripting vulnerability has been reported in 'A2Z.JSP' due to insufficient sanitization of the 'kwd' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	LogMethods Cross-Site Scripting CVE-2006-2000	2.3	Security Focus, Bugtraq ID: 17675, April 24, 2006
DC Scripts DCForum 3.0	Multiple input validation vulnerabilities have been reported in 'DCBoard.cgi' include Cross-Site Scripting and SQL injection due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, dcforumlite-3.0-sql-xss.txt, has been published.	DCForum Multiple Input Validation CVE-2006-2049 CVE-2006-2050	Not Available	Security Focus, Bugtraq ID: 17697, April 25, 2006
DeleGate DeleGate 8.11.5 & prior (stable), 9.0.5 & prior (development)	A remote Denial of Service vulnerability has been reported due to a failure to properly handle malformed DNS query packets. Updates available Currently we are not aware of any exploits for this vulnerability.	DeleGate DNS Query Handling Remote Denial of Service	Not Available	Secunia Advisory: SA19750, April 26, 2006
dForum dForum 1.5 & prior	File include vulnerabilities have been reported due to insufficient verification of the 'DFORUM_PATH' parameter in various scripts, which could let a remote malicious user execute arbitrary PHP files. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	dForum Multiple Remote File Include CVE-2006-1994	7.0	Security Focus, Bugtraq ID: 17650, April 22, 2006
DIA DIA 0.87-0.94	Multiple remote buffer overflow vulnerabilities have been reported due to a failure to properly bounds-check user-supplied input before copying it into insufficiently sized memory buffers, which could let a remote malicious user execute arbitrary code. The vendor has released version 0.95-pre6, along with a patch for 0.94 to address these issues. Mandriva Ubuntu Fedora Debian **Gentoo** Currently we are not aware of any exploits for these vulnerabilities.	DIA XFIG File Import Multiple Remote Buffer Overflows CVE-2006-1550	5.6	Security Focus, Bugtraq ID: 17310, March 29, 2006 Mandriva Security Advisory, MDKSA-2006:062, April 3, 2006 Debian Security Advisory, DSA-1025-1, April 6, 2006 **Gentoo Linux Security Advisory, GLSA 200604-14, April 23, 2006**
DUware DUportal Pro 3.4	An SQL injection vulnerability has been reported in 'cat.asp' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, DUportalPro-cat.asp-sql.txt, has been published.	DUWare DUPortal Pro SQL Injection	Not Available	Security Focus, Bugtraq ID: 17702, April 26, 2006
Help Center Live Help Center Live 2.0, 1.2- 1.2.8, 1.0	Multiple SQL injection vulnerabilities have been reported in the 'osTicket' module due to insufficient sanitization of unspecified parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available Vulnerabilities can be exploited through a web client.	Help Center Live OSTicket Module Multiple SQL Injection CVE-2006-2039	Not Available	Secunia Advisory: SA19776, April 24, 2006

Instant Photo Gallery Instant Photo Gallery 1.0	A Cross-Site Scripting and SQL injection vulnerability has been reported in 'portfolio_photo_ popup.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, instantphotogallery-xss.txt, has been published.	Instant Photo Gallery Cross-Site Scripting & SQL Injection CVE-2006-2052	Not Available	Secunia Advisory: SA19813, April 26, 2006
Invision Power Services Invision Board 2.0-2.1.5	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'search.php' due to insufficient sanitization of the 'lastdate' parameter before using in a 'preg_replace()' call, which could let a remote malicious user execute arbitrary PHP code; an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'ck' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'admin.php' because it is possible for administrators to include arbitrary PHP scripts via the 'name' parameter, which could lead to the execution of arbitrary PHP code; and a vulnerability was reported because it is possible to upload a malicious JPEG image with a GIF header, which could let a remote malicious user execute arbitrary HTML and script code. Patches available Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, invisionpowerboard-2.1.5-sql-inj.txt, has been published.	Invision Power Board Multiple Vulnerabilities CVE-2006-2059 CVE-2006-2060 CVE-2006-2061	Not Available	Secunia Advisory: SA19830, April 26, 2006
IP3 Networks NA75 4.0.34 firmware	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input passed to the web interface before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported due to input validation errors in the command line interface, which could let a remote malicious user inject arbitrary shell commands; a vulnerability was reported because the shadow password file has world-readable permissions, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported because the database file is stored with world-readable and world-writable permissions. Patch available Currently we are not aware of any exploits for these vulnerabilities.	IP3 Networks NA75 Multiple Vulnerabilities CVE-2006-2043 CVE-2006-2044 CVE-2006-2045	Not Available	Secunia Advisory: SA19818. April 26, 2006
I-RATER I-RATER Platinum 0	A file include vulnerability has been reported in 'common.php' due to insufficient verification of the 'include_path' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	I-RATER Platinum Remote File Include CVE-2006-1929	2.3	Security Focus, Bugtraq ID: 17623, April 20, 2006
Juniper Networks JUNOSe 5.x, 6.x, 7.x	A remote Denial of Service vulnerability has been reported due to a failure to properly handle DNS datagrams. The vendor has released updated versions of the affected software to address this issue. Currently we are not aware of any exploits for this vulnerability.	Juniper JUNOSe DNS Client Remote Denial of Service	Not Available	Security Focus, Bugtraq ID: 17693, April 25, 2006

kcscripts.com Portal Pack 6.0	Cross-Site Scripting vulnerabilities have been reported in 'calendar/Visitor.cgi' and 'news/NsVisitor.cgi' due to insufficient sanitization of the 'sort_order' parameter, in 'search/search.cgi' due to insufficient sanitization of the 'q' parameter, and in 'classifieds/viewcat.cgi' due to insufficient sanitization of the 'cat_id' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploit scripts have been published.	Portal Pack Multiple Cross-Site Scripting CVE-2006-1967 CVE-2006-1968 CVE-2006-1969 CVE-2006-1970	1.9 (CVE-2006-1967) 4.7 (CVE-2006-1968) 1.9 (CVE-2006-1969) 2.3 (CVE-2006-1970)	Secunia Advisory: SA19695, April 20, 2006
Manic Web MWGuest 2.1	An HTML injection vulnerability has been reported in 'MWguest.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Manic Web MWGuest HTML Injection CVE-2006-1979	4.7	Security Focus, Bugtraq ID: 17630, April 20, 2006
Michael Romedahl RI Blog 1.1	SQL injection vulnerabilities have been reported due to insufficient sanitization of the 'Username' and 'Password' fields during login, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	RI Blog Multiple SQL Injection CVE-2006-2004	7.0	Security Focus, Bugtraq ID: 17654, April 22, 2006
MiniNuke MiniNuke CMS 1.8.2 & prior	An SQL injection vulnerability has been reported in 'pages.asp' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Mini-NUKE SQL Injection CVE-2006-0870	7.0	Security Focus, Bugtraq ID: 17636, April 20, 2006
MKPortal MKPortal 1.1 RC1	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'include/VB/vb_board_ functions.php' script due to insufficient validation of several parameters, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in the 'includes/pm_popup.php' script due to insufficient filtering of HTML code from user-supplied input before displaying, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	MKPortal Cross-Site Scripting & SQL Injection CVE-2006-2066 CVE-2006-2067	Not Available	Security Tracker Alert ID: 1015977, April 22, 2006
Mozilla. org Mozilla Browser prior to 1.7.13, Seamonkey prior to 1.0.1, Thunderbird prior to 1.0.8, 1.5 - 1.5.0.1, Firefox, 1.5 - 1.5.0.1	A vulnerability has been reported in the 'crypto.generate CRMFRequest' method, which could let a remote malicious user execute arbitrary code. Updates available Fedora RHSA-2006-0328.html RHSA-2006-0329.html **Ubuntu** **SuSE** **Gentoo** **MDKSA-2006:075** **Slackware** **SGI**	Mozilla Browser Suite 'crypto.generate CRMFRequest' Arbitrary Code Execution CVE-2006-1728	7.0	Security Tracker Alert IDs: 1015922, 1015923, 1015924, 015925, April 14, 2006 RedHat Security Advisories, RHSA-2006-0328 & 0329, April 14 & 18, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#932734 **Ubuntu Security Notice, USN-271-1 April 19, 2006** **SuSE Security Announcement, SUSE-SA:2006:021, April 20, 2006**

	RHSA-2006-0330 **MDKSA-2006:078** **SUSE-SA:2006:022** Currently we are not aware of any exploits for this vulnerability.			**Gentoo Linux Security Advisory, GLSA 200604-12, April 23, 2006** **Mandriva Security Advisory, MDKSA-2006:075, April 24, 2006** **Slackware Security Advisory, SSA:2006-114-01, April 24, 2006** **SGI Security Advisory, 20060404-01-U, April 24, 2006** **RedHat Security Advisory, RHSA-2006:0330-15, April 25, 2006** **Mandriva Security Advisory, MDKSA-2006:078, April 25, 2006** **SuSE Security Announcement, SUSE-SA:2006:022, April 25, 2006**
Mozilla.oeg Thunderbird prior to 1.0.8, 1.5 - 1.5.0.1; Seamonkey prior to 1.0.1; Mozilla browser prior to 1.7.13; Firefox prior to 1.0.8, 1.5 - 1.5.0.1	A integer overflow vulnerability has been reported because a remote malicious user can create an HTML based email that contains a specially crafted CSS letter-spacing property value, which could lead to the execution of arbitrary code. Updates available RHSA-2006-0328.html RHSA-2006-0329.html **Ubuntu** **SuSE** **Gentoo** **MDKSA-2006:075** **Slackware** **SGI** **RHSA-2006-0330** **MDKSA-2006:078** **SUSE-SA:2006:022** Currently we are not aware of any exploits for this vulnerability.	Mozilla Integer Overflow CVE-2006-1730	7.0	Security Tracker Alert IDs: 1015915, 1015916, 1015917, 1015918, April 14, 2005 RedHat Security Advisories, RHSA-2006-0328 & 0329, April 14 & 18, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#179014 **Ubuntu Security Notice, USN-271-1 April 19, 2006** **SuSE Security Announcement, SUSE-SA:2006:021, April 20, 2006** **Gentoo Linux Security Advisory, GLSA 200604-12, April 23, 2006** **Mandriva Security Advisory, MDKSA-2006:075, April 24, 2006** **Slackware Security Advisory, SSA:2006-114-01, April 24, 2006** **SGI Security Advisory, 20060404-01-U, April 24, 2006** **RedHat Security Advisory, RHSA-2006:0330-15, April 25, 2006** **Mandriva Security Advisory, MDKSA-2006:078, April**

	25, 2006 SuSE Security Announcement, SUSE-SA:2006:022, April 25, 2006

Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'Install Trigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for a remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available Gentoo Mandriva Fedora RedHat Slackware Ubuntu Ubuntu Ubuntu SUSE Debian Debian SGI Gentoo Slackware Debian Debian Fedora HP HP Ubuntu Sun SUSE Mandriva **SUSE-SA:2006:022** Exploits have been published.	Firefox Multiple Vulnerabilities CVE-2005-2260 CVE-2005-2261 CVE-2005-2262 CVE-2005-2263 CVE-2005-2264 CVE-2005-2265 CVE-2005-2267 CVE-2005-2269 CVE-2005-2270	8.0 (CVE-2005-2260) 7.0 (CVE-2005-2261) 4.5 (CVE-2005-2262) 3.3 (CVE-2005-2263) 9.0 (CVE-2005-2264) 3.3 (CVE-2005-2265) 7.0 (CVE-2005-2267) 7.0 (CVE-2005-2269) 7.0 (CVE-2005-2270)	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security Advisory, SSA:2005-085-01, August 28, 2005 Debian Security Advisory, DSA 779-2, September 1, 2005

				Debian Security Advisory, DSA 810-1, September 13, 2005 Fedora Legacy Update Advisory, FLSA:160202, September 14, 2005 HP Security Bulletin, HPSBOV01229, September 19, 2005 HP Security Bulletin, HPSBUX01230, October 3, 2005 Ubuntu Security Notice, USN-155-3, October 04, 2005 Sun(sm) Alert Notification Sun Alert ID: 101952, October 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005 Mandriva Linux Security Advisory, MDKSA-2005:226, December 12, 2005 **SuSE Security Announcement, SUSE-SA:2006:022, April 25, 2006**
Mozilla.org Firefox 1.5-1.5.2, 1.5.0.2	A buffer overflow vulnerability has been reported in the 'iframe.contentWindow.focus()' function due to improper processing of certain JavaScript code, which could let a remote malicious user cause a Denial or Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script, ffdos.txt, has been published.	Mozilla Firefox 'iframe.content Window.focus()' Buffer Overflow CVE-2006-1993	3.7	Security Tracker Alert ID: 1015981, April 24, 2006
Multiple Vendors Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11; Netscape Browser 8.0.3.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability was reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks. Firefox Mozilla Browser RedHat Ubuntu Mandriva	Mozilla Browser / Firefox Multiple Vulnerabilities CVE-2005-2701 CVE-2005-2702 CVE-2005-2703 CVE-2005-2704 CVE-2005-2705 CVE-2005-2706 CVE-2005-2707	7.0 (CVE-2005-2701) 8.0 (CVE-2005-2702) 3.3 (CVE-2005-2703) 3.3 (CVE-2005-2704) 7.0 (CVE-2005-2705) 4.7 (CVE-2005-2706) 3.3 (CVE-2005-2707)	Mozilla Foundation Security Advisory, 2005-58, September 22, 2005 RedHat Security Advisory, RHSA-2005:789-11, September 22, 2005 Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 SGI Security Advisory, 20050903-02-U, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1017,

	Fedora Slackware SGI Conectiva Gentoo SUSE Fedora Debian TurboLinux Mandriva Ubuntu Netscape Debian Debian FedoraLegacy **SuSE** Currently we are not aware of any exploits for these vulnerabilities.			September 28, 2005 Gentoo Linux Security Advisory [UPDATE], September 29, 2005 SUSE Security Announcement, SUSE-SA:2005:058, September 30, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Debian Security Advisory, DSA 838-1, October 2, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005 Ubuntu Security Notice, USN-200-1, October 11, 2005 Security Focus, Bugtraq ID: 14916, October 19, 2005 Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005 Fedora Legacy Update Advisory, FLSA:168375, January 9, 2006 **SuSE Security Announcement, SUSE-SA:2006:022, April 25, 2006**
Multiple Vendors Mozilla Browser 0.8-0.9.9, 0.9.35, 0.9.48, 1.0-1.7.12, Thunderbird 0.x, 1.x, Firefox 0.x, 1.x; SeaMonkey 1.0; RedHat Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, ES 2.1, AS 4, AS 3, AS 2.1 IA64, AS 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1	Multiple vulnerabilities have been reported: vulnerabilities were reported because temporary variables that are not properly protected are used in the JavaScript engine's garbage collection, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported because a remote malicious user can create HTML that will dynamically change the style of an element from position:relative to position:static; a vulnerability was reported because a remote malicious user can create HTML that invokes the QueryInterface() method of the built-in Location and Navigator objects; a vulnerability was reported in the 'XULDocument.persist()' function due to improper validation of the user-supplied attribute name, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability was reported in the 'E4X,' 'SVG,' and 'Canvas' features, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the XML parser because data can be read from locations beyond the end of the buffer, which could lead to a Denial of Service; and a vulnerability was reported because the 'E4X' implementation's internal 'AnyName' object is incorrectly available to web content, which could let a remote malicious user bypass same-origin restrictions. Mozilla RedHat RedHat Fedora Mandriva	Multiple Mozilla Products Vulnerabilities CVE-2006-0292 CVE-2006-0293 CVE-2006-0294 CVE-2006-0295 CVE-2006-0296 CVE-2006-0297 CVE-2006-0298 CVE-2006-0299	7.0 (CVE-2006-0292) 7.0 (CVE-2006-0293) 7.0 (CVE-2006-0294) 3.9 (CVE-2006-0295) 2.3 (CVE-2006-0296) 3.9 (CVE-2006-0297) 2.3 (CVE-2006-0298) 4.7 (CVE-2006-0299)	Mozilla Foundation Security Advisories 2006-01-2006-08, February 1, 2006 RedHat Security Advisories, RHSA-2006:0199-10 & RHSA-2006:0200-8, February 2, 2006 Fedora Security Advisories, FEDORA-2006-075 & FEDORA-2006-076, February 2, 2006 US-CERT VU#592425 US-CERT VU#759273 Mandriva Security Advisories, MDKSA-2006:036 & MDKSA-2006:037, February 7, 2006 SGI Security Advisory, 20060201-01-U, March 14, 2006 **Ubuntu Security Notice, USN-271-1 April 19, 2006** **Gentoo Linux Security Advisory, GLSA**

	Mandriva SGI **Ubuntu** **Gentoo** **RHSA-2006-0330** **MDKSA-2006:078** **SUSE-SA:2006:022** There is no exploit code required for some of these vulnerabilities; however, an exploit, firefox_queryinterface.pm, has been published.			**200604-12, April 23, 2006** **RedHat Security Advisory, RHSA-2006:0330-15, April 25, 2006** **Mandriva Security Advisory, MDKSA-2006:078, April 25, 2006** **SuSE Security Announcement, SUSE-SA:2006:022, April 25, 2006**
Multiple Vendors RedHat Fedora Core5; Ethereal Group Ethereal 0.10-0.10.14, 0.9-0.9.16, 0.8.5	Multiple vulnerabilities have been reported vulnerabilities due to various types of errors including boundary errors, an off-by-one error, an infinite loop error, and several unspecified errors in a multitude of protocol dissectors, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Updates available Mandriva Fedora Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Protocol Dissector Vulnerabilities CVE-2006-1932 CVE-2006-1933 CVE-2006-1934 CVE-2006-1935 CVE-2006-1936 CVE-2006-1937 CVE-2006-1938 CVE-2006-1939 CVE-2006-1940	4.9 (CVE-2006-1932) 2.3 (CVE-2006-1933) 2.3 (CVE-2006-1934) 2.3 (CVE-2006-1935) 2.3 (CVE-2006-1936) 2.3 (CVE-2006-1937) 2.3 (CVE-2006-1938) 2.3 (CVE-2006-1939) 2.3 (CVE-2006-1940)	Secunia Advisory: SA19769, April 25, 2006 Mandriva Security Advisory, MDKSA-2006:077, April 25, 2006

Multiple Vendors Slackware Linux 10.2, -current; RedHat Fedora Core5, Core4, Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Netscape 7.2, Netscape Browser 8.0.4; Mozilla Thunderbird 1.5.1, 1.5 Beta 2, 1.5, 1.0-1.0.7, 0.9, 0.8, 0.7-0.7.3, 0.6; Mozilla SeaMonkey 1.0 dev, 1.0; Mozilla Firefox 1.5.1, 1.5 beta 1 & beta2, 1.5, 1.0-1.0.7, 0.10.1, 0.10, 0.9-0.9.3, 0.8, Firefox Preview Release; Mozilla Browser 1.8 Alpha 1 - Alpha 4, Mozilla Browser 1.8 Alpha 3 Mozilla Browser 1.8 Alpha 2 Mozilla Browser 1.8 Alpha 1 Mozilla Browser 1.7-1.7.12, 1.6, 1.5.1, 1.5, 1.4.4, 1.4.2, 1.4.1, 1.4 b, 1.4 a, 1.4 , 1.3.1, 1.3, 1.2.1, 1.2 Alpha & Beta, 1.2, 1.1 Alpha & Beta, 1.1, 1.0-1.0.2, 0.9.48, 0.9.35, 0.9.9, 0.9.2-0.9.8, M16, M15	Multiple vulnerabilities have been reported which could lead to the execution of arbitrary code, cause a Denial or Service, elevated privileges, execution of arbitrary JavaScript code, disclosure of sensitive information, bypass security restrictions, or spoofing of windows contents. New versions of the Mozilla Suite, Firefox, SeaMonkey, and Thunderbird are available to address these issues. Fedora RHSA-2006-0328.html RHSA-2006-0329.html **Ubuntu** **SuSE** **Gentoo** **MDKSA-2006:075** **Slackware** **SGI** **RHSA-2006-0330** **MDKSA-2006:078** **SUSE-SA:2006:022** Some of these vulnerabilities do not require exploit code.	Mozilla Suite, Firefox, SeaMonkey, & Thunderbird Multiple Remote Vulnerabilities CVE-2006-1729 CVE-2006-1045 CVE-2006-0748 CVE-2006-1725 CVE-2006-1731 CVE-2006-0749 CVE-2006-1732 CVE-2006-1733 CVE-2006-1734 CVE-2006-1735 CVE-2006-1736 CVE-2006-1737 CVE-2006-1738 CVE-2006-1739 CVE-2006-1740 CVE-2006-1741 CVE-2006-1742 CVE-2006-1790	2.3 (CVE-2006-1729) 1.9 (CVE-2006-1045) 7.0 (CVE-2006-0748) 7.0 (CVE-2006-0749) 1.9 (CVE-2006-1725) 1.9 (CVE-2006-1731) 2.3 (CVE-2006-1732) 7.0 (CVE-2006-1733) 7.0 (CVE-2006-1734) 7.0 (CVE-2006-1735) 1.9 (CVE-2006-1736) 7.0 (CVE-2006-1737) 2.3 (CVE-2006-1738) 7.0 (CVE-2006-1739) 1.9 (CVE-2006-1740) 2.3 (CVE-2006-1741) 2.3 (CVE-2006-1742) 7.0 (CVE-2006-1790)	Security Focus, Bugtraq ID: 17516, April 18, 2006 RedHat Security Advisories, RHSA-2006-0328 & 0329, April 14 & 18, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#935556 US-CERT VU#492382 US-CERT VU#736934 US-CERT VU#813230 US-CERT VU#842094 US-CERT VU#488774 **Ubuntu Security Notice, USN-271-1 April 19, 2006** **SuSE Security Announcement, SUSE-SA:2006:021, April 20, 2006** **Gentoo Linux Security Advisory, GLSA 200604-12, April 23, 2006** **Mandriva Security Advisory, MDKSA-2006:075, April 24, 2006** **Slackware Security Advisory, SSA:2006-114-01, April 24, 2006** **SGI Security Advisory, 20060404-01-U, April 24, 2006** **RedHat Security Advisory, RHSA-2006:0330-15, April 25, 2006** **Mandriva Security Advisory, MDKSA-2006:078, April 25, 2006** **SuSE Security Announcement, SUSE-SA:2006:022, April 25, 2006**
My Gaming Ladder My Gaming Ladder 7.0	A file include vulnerability has been reported in 'stats.php' due to insufficient verification of the 'dir[base]' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, 17657-exploit.pl, has been published.	My Gaming Ladder Remote File Include CVE-2006-2002	2.3	Secunia Advisory: SA19773, April 24, 2006
MyBB DevBB 1.0	A Cross-Site Scripting vulnerability has been reported in 'Member.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, DevBB-1.0.0-xss.txt, has been published.	DevBB Cross-Site Scripting CVE-2006-2070	Not Available	Security Focus, Bugtraq ID: 17703, April 26, 2006

NextAge NextAge Shopping Cart 0	Multiple HTML injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using it in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, nextage-html-inj.txt, has been published.	NextAge Shopping Cart Multiple HTML Injection CVE-2006-2051	Not Available	Security Focus, Bugtraq ID: 17685, April 25, 2006
OpenTTD OpenTTD 0.4.7, 0.4 .0.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the 'PACKET_SERVER_ERROR' and 'PACKET_CLIENT_ERROR' command packets due to an error; and a vulnerability was reported due to an error when handling the packet size field in a received UDP. The vulnerability has reportedly been fixed in revision r4531 in the CVS repositories. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, openttdx.zip, has been published.	OpenTTD Remote Denials of Service CVE-2006-1999 CVE-2006-1998	2.3 (CVE-2006-1999) 1.6 (CVE-2006-1998)	Security Focus, Bugtraq ID: 17661, April 24, 2006
Oracle JD Edwards EnterpriseOne 8.x, OneWorld 8.x, Oracle Application Server 10g, Collaboration Suite 10.x, Database 10g, 8.x, E-Business Suite 11i, Enterprise Manager 10.x, PeopleSoft Enterprise Tools 8.x, Pharmaceutical Applications 4.x, Workflow 11.x, Oracle9i Application Server, Oracle9i Collaboration Suite, Oracle9i Database Enterprise Edition, Standard Edition, Oracle9i Developer Suite	Oracle has released a Critical Patch Update advisory for April 2006 to address multiple vulnerabilities. Some have an unknown impact, and others can be exploited to conduct SQL injection attacks. Patch information Currently we are not aware of any exploits for these vulnerabilities.	Oracle Products Multiple Vulnerabilities	Not Available	Oracle Security Advisory, April 18, 2006 Technical Cyber Security Alert TA06-109A US-CERT VU#241481 US-CERT VU#240249 **US-CERT VU#443265** **US-CERT VU#879041** **US-CERT VU#549146** **US-CERT VU#452681** **US-CERT VU#797465** **US-CERT VU#139049** **US-CERT VU#824833** **US-CERT VU#940729** **US-CERT VU#619194**
PCPIN PCPIN Chat 5.0.4 & prior	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'main.php' due to insufficient sanitization of the 'login' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a file include vulnerability was reported in 'main.php' due to insufficient verification of the 'language' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, an exploit script, PCPIN_Chat-5.0.4_ RCE.php, has been published.	PCPIN Chat SQL Injection & File Include CVE-2006-1962 CVE-2006-1963	7.0 (CVE-2006-1962) 2.8 (CVE-2006-1963)	Security Tracker Alert ID: 1015968, April 20, 2006
Photokorn Photokorn 1.542, 1.53	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, photokorn-1.53-sql.txt, has been published.	Photokorn Multiple SQL Injection CVE-2006-2040	Not Available	Security Focus, Bugtraq ID: 17683, April 25, 2006

PHP Group PHP 4azdgvote .x, 4.2.x, 4.3.x, 4.4.x, 5.0.x, 5.1.x	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function because only the first 4096 characters of an array request parameter are sanitized before returning to users, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability was reported in the 'tempnam()' PHP function due to an error, which could let a remote malicious create arbitrary files; a vulnerability was reported in the 'copy()' PHP function due to an error, which could let a remote malicious create arbitrary files; and a vulnerability was reported in the 'copy()' PHP function because the safe mode mechanism can be bypassed by a remote malicious user. Updates available **MDKSA-2006:074** **RHSA-2006-0276** Vulnerabilities may be exploited with standard PHP code; however, Proof of Concept exploit scripts have been published.	PHP Multiple Vulnerabilities CVE-2006-0996 CVE-2006-1494 CVE-2006-1608	1.9 (CVE-2006-0996) 1.9 (CVE-2006-1494) 1.6 (CVE-2006-1608)	Secunia Advisory: SA19599, April 10, 2006 **Mandriva Security Advisory, MDKSA-2006:074, April 24, 2006** **RedHat Security Advisory, RHSA-2006:0276-9, April 25, 2006**
PHP Group PHP 4.3.x, 4.4.x, 5.0.x, 5.1.x	A vulnerability has been reported in the 'html_entity_decode()' function because it is not binary safe, which could let a remote malicious user obtain sensitive information. The vulnerability has been fixed in the CVS repository and in version 5.1.3-RC1. Mandriva Trustix **RHSA-2006-0276** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Information Disclosure CVE-2006-1490	2.3	Secunia Advisory: SA19383, March 29, 2006 Mandriva Security Advisory, MDKSA-2006:063, April 2, 2006 Trustix Secure Linux Security Advisory #2006-0020, April 7, 2006 **RedHat Security Advisory, RHSA-2006:0276-9, April 25, 2006**
PHP Group PHP 4.4.2, 5.1.2	A buffer overflow vulnerability has been reported in the 'wordwrap()' function in 'string.c' when calculating an integer value based on user-supplied input, which could let a remote malicious user cause a Denial or Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHP 'wordwrap()' Buffer Overflow CVE-2006-1990	2.3	Security Tracker Alert ID: 1015979, April 24, 2006
PHP PHP 5.1.1, 5.1	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient of the session ID in the session extension before returning to the user, which could let a remote malicious user inject arbitrary HTTP headers; a format string vulnerability was reported in the 'mysqli' extension when processing error messages, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insufficient sanitization of unspecified input that is passed under certain error conditions, which could let a remote malicious user execute arbitrary HTML and script code. PHP Mandriva Ubuntu Gentoo **RHSA-2006-0276** There is no exploit code required.	Multiple PHP Vulnerabilities CVE-2006-0207 CVE-2006-0208	2.3 (CVE-2006-0208)	Secunia Advisory: SA18431, January 13, 2006 Mandriva Security Advisory, MDKSA-2006:028, February 1, 2006 Ubuntu Security Notice, USN-261-1, March 10, 2006 Gentoo Linux Security Advisory, GLSA 200603-22, March 22, 2006 **RedHat Security Advisory, RHSA-2006-0276, April 25, 2006**

PHP Surveyor PHPSurveyor 0.995	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'save.php' script due to insufficient sanitization of the 'surveyid' cookie parameter, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported because a remote malicious user can cause the system to write arbitrary PHP code to a file No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, phpsurveror.php, has been published.	PHPSurveyor Input Validation CVE-2006-2065	Not Available	Security Tracker Alert ID: 1015970, April 20, 2006
phpldapadmin phpldapadmin 0.9.8	Several vulnerabilities have been reported: an HTML injection vulnerability was reported due to insufficient sanitization of 'compare_form.php,' ' copy_form.php,' 'rename_form.php,' 'template_engine.php,' 'delete_form.php,' and 'search.php,' which could let a remote malicious user execute arbitrary HTML and script code: and a Cross-Site Scripting vulnerability was reported in 'template_engine.php' due to insufficient sanitization of the 'Container DN,' 'Machine Name, ' and 'UID Number' parameters before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, 17643.html, has been published.	PHPLDAPAdmin Multiple Input Validation CVE-2006-2016	1.9	Secunia Advisory: SA19747, April 21, 2006
phpMy Agenda phpMyAgenda 3.0 Final & prior	A file include vulnerability has been reported in 'agenda.php3' due to insufficient sanitization of the 'rootagend' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, phpMyAgenda_fi.txt, has been published.	PHPMyAgenda Remote File Include CVE-2006-2009	7.0	Security Tracker Alert ID: 1015984, April 24, 2006
PHP PHP 5.0 .0- 5.0.5, 4.4.1, 4.4 .0, 4.3-4.3.11, 4.2-4.2.3, 4.1.0-4.1.2, 4.0.6, 4.0.7, RC1-RC3	A vulnerability has been reported in the 'mb_send_mail()' function due to an input validation error, which could let a remote malicious user inject arbitrary headers to generated email messages. Upgrades available SUSE Ubuntu Mandriva **RHSA-2006-0276** There is no exploit code required.	PHP MB_Send_Mail Arbitrary Header Injection CVE-2005-3883	2.3	Security Focus, Bugtraq ID: 15571, November 25, 2005 SUSE Security Announcement, SUSE-SA:2005:069, December 14, 2005 Ubuntu Security Notice, USN-232-1, December 23, 2005 Mandriva Linux Security Advisory, MDKSA-2005:238, December 27, 2005 **RedHat Security Advisory, RHSA-2006-0276, April 25, 2006**
PhpWeb Gallery PhpWeb Gallery 1.x	A vulnerability has been reported in 'picture.php' because it is possible to disclose arbitrary pictures by not defining a value for the 'cat' parameter, which could let a remote malicious user obtain sensitive information. The vulnerability has been fixed in version 1.6.0RC1. Currently we are not aware of any exploits for this vulnerability.	PhpWebGallery Arbitrary Picture Disclosure CVE-2006-2041	Not Available	Secunia Advisory: SA19801, April 25, 2006
phpWebFTP phpWebFTP 2.3	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input using the HTTP 'POST' method when submitting a malicious URI, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script,	PHPWebFTP Multiple Cross-Site Scripting CVE-2006-2048	Not Available	Security Focus, Bugtraq ID: 17688, April 25, 2006

	phpwebftp-2.3-xss.txt, has been published.			
Plexum PlexCart X5 & prior	SQL injection vulnerabilities have been reported in 'plexum.php' due to insufficient sanitization of the 'pagesize,' 'maxrec,' 'startpos' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploit scripts have been published.	Plexum Multiple SQL Injection CVE-2006-1947 CVE-2006-1949	7.0 (CVE-2006-1947) 7.0 (CVE-2006-1949)	Security Focus, Bugtraq ID: 17617, April 20, 2006
Scry Gallery Scry Gallery 0	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in the 'index.php' script due to insufficient validation of the 'p' field, which could let a remote malicious user obtain sensitive information; and a path disclosure vulnerability was reported in the 'p' field due to an input validation error when processing a non-existing directory, which could let a remote malicious user obtain sensitive information. The vendor has released an update to address this issue. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, 17649-directory-traversal.exploit, has been published.	Scry Gallery Directory Traversal & Path Disclosure CVE-2006-1995 CVE-2006-1996	2.3 (CVE-2006-1995) 2.3 (CVE-2006-1996)	Moroccan Security Team Advisory , April 21, 2006
Scry Gallery Scry Gallery 1.1	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, scry_xss.txt, has been published.	Scry Gallery Cross-Site Scripting CVE-2006-2001	2.3	Security Focus, Bugtraq ID: 17668, April 21, 2006
Sebastien Lecluse SL_site 1.0	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'page.php' due to insufficient sanitization of the 'id_page' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Directory Traversal vulnerability was reported in 'gallerie.php' due to insufficient sanitization of the 'rep' parameter before using to list images, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability was reported in 'recherche.php' due to insufficient sanitization of the 'recherche' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	SL_site Multiple Vulnerabilities CVE-2006-2013 CVE-2006-2014 CVE-2006-2015	7.0 (CVE-2006-2013) 2.3 (CVE-2006-2014) 1.9 (CVE-2006-2015)	Secunia Advisory: SA19792, April 24, 2006
Simplog Simplog 0.9.1-0.9.3	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported in 'archive.php' due to insufficient sanitization of the 'cid,' 'pid,' and 'eid' parameters, in 'preview.php' due to insufficient sanitization of the 'tid' parameter, and in 'comments.php' due to insufficient sanitization of the 'pid' parameter, which could let a remote malicious user execute arbitrary SQL code; and Cross-Site Scripting vulnerabilities were reported in 'imagelist.php' due to insufficient sanitization of the 'imagedir' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Vulnerabilities can be exploited through a web client; however, Proof of Concept exploit scripts, 17652.html, and 17652-exploit.pl, have been published.	Simplog SQL Injection & Cross-Site Scripting CVE-2006-2028 CVE-2006-2029	Not Available	Secunia Advisory: SA19764 , April 24, 2006

Symantec AntiVirus Scan Engine 5.0.0.24	Multiple vulnerabilities have been reported: a vulnerability was reported in the authentication mechanism due a design error, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a static private DSA key is used for SSL communications, which could let a remote malicious user conduct man-in-the-middle attacks; and a vulnerability was reported due to insufficient access restriction to files in the installation directory, which could let a remote malicious user obtain sensitive information. Update information An exploit script, change_scan_engine_pw.pl, has been published for the authentication bypass vulnerability.	Symantec Scan Engine Multiple Vulnerabilities CVE-2006-0230 CVE-2006-0231 CVE-2006-0232	10.0 (CVE-2006-0230) 4.7 (CVE-2006-0231) 2.3 (CVE-2006-0232)	Symantec Security Advisory, SYM06-008 , April 21, 2006
Thwboard Thwboard 3.0 Beta 2.84	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	ThWboard Cross-Site Scripting CVE-2006-2037	Not Available	Security Focus, Bugtraq ID: 17627, April 20, 2006
W2B Online Banking 0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'sid' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	W2B Online Banking Cross-Site Scripting CVE-2006-1980	1.9	Security Focus, Bugtraq ID: 17626, April 20, 2006
WingNut EasyGallery 1.17	A Cross-Site Scripting vulnerability has been reported in 'EasyGallery.PHP' due to insufficient sanitization of the 'ordner' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	EasyGallery Cross-Site Scripting CVE-2006-1972	2.3	Security Focus, Bugtraq ID: 17624, April 20, 2006
WWWThreads WWWThreads RC3	SQL injection vulnerabilities have been reported in 'message_list.php' due to insufficient sanitization of the 'messages' parameter and in 'register.php' due to insufficient sanitization of the 'referral_id' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	WWWThread Multiple SQL Injection CVE-2006-1958	4.7	Security Focus, Bugtraq ID: 17615, April 20, 2006

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Bringing More Security to Wi-Fi Networks: According to the research director for Gartner, protecting enterprise Wi-Fi networks from intrusions is a big challenge, but IT has a growing arsenal of products available to help, including those based on the 2004 Wi-Fi security standard (the IEEE's 802.11i) and the Wi-Fi Alliance's closely related implementation protocol, WPA2 (the Wi-Fi Protected Access 2). Advanced encryption and authentication mechanisms make these specs "actually more secure than most wired networks."
- Bluetooth virus leaves mobile users out of pocket: Security experts warned at Infosec Europe 2006, that a newly detected mobile phone virus is charging mobile phone users $5 to send a premium rate SMS message. According to F-Secure, a Proof of Concept attack has been reengineered to make money illegally from mobile phone users. "The virus gets your phone to send an SMS to a premium rate number and then sends an authority that they can charge you without you knowing about it," said Richard Hales, country manager for UK and Ireland at F-Secure.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Asia Now Top Spam-Relaying Region: According to a report released by Sophos, Asia has overtaken North America to become the top spam-relaying region in the world. Nearly one-half the spam Sophos captured on its global spam-monitoring network originated in Asia, with North America coming in a distant second as the source of just over 25 percent of spam. As recently as two years ago, the U.S. was responsible for the majority of spam sent around the world, said Graham Cluley, senior technology consultant for Sophos.
- Hacker's Toolkit Attacks Unpatched Computers**:** According to an online alert from Websense, a dirt-cheap, do-it-yourself hacking kit sold by a Russian Web site is being used by more than 1,000 malicious Web sites. Those sites have confiscated hundreds of thousands of computers using the "smartbomb" kit, which sniffs for seven unpatched vulnerabilities in Internet Explorer and Firefox, then attacks the easiest-to-exploit weakness.
- Weak passwords leave firms open to hackers**:** According to a survey published at Infosec Europe 2006, poor password policy management is leaving firms open to hacking attacks. Nearly two thirds of the 500 IT administrators who responded to the poll considered the passwords of their users to be inadequate, either using common dictionary words, names or other weak passwords.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
5	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
6	Nyxum-D	Win32 Worm	Stable	March 2006	A mass-mailing worm that turns off anti-virus, deletes files, downloads code from the internet, and installs in the registry. This version also harvests emails addresses from the infected machine and uses its own emailing engine to forge the senders address.
7	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
8	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
9	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
10	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.

Table updated April 25, 2006

[back to top]

Last updated April 27, 2006